

COMMAND ALKON INCORPORATED – NACHTRAG ZUR DATENVERARBEITUNG

Aktualisiert: 31.07.25

Dieser Zusatz zur Datenverarbeitung („DPA“) ist Bestandteil der *Rahmenlizenz- und Dienstleistungsvereinbarung* („Vereinbarung“) zwischen: (i) dem Kunden (in der Rahmenlizenz- und Dienstleistungsvereinbarung genannt) und seinen verbundenen Unternehmen („Kunde“) und (ii) Command Alkon Incorporated und seinen verbundenen Unternehmen („Unternehmen“), sofern dies gemäß der Datenschutz-Grundverordnung („DSGVO“) oder anderen geltenden Datenschutzgesetzen erforderlich ist.

Dieser DPA ersetzt alle früheren Vereinbarungen zwischen den Parteien über den Gegenstand dieser Vereinbarung, d. h. den Datenschutz und die Datensicherheit gemäß den Datenschutzgesetzen (wie unten definiert).

Unter Berücksichtigung der hierin festgelegten gegenseitigen Verpflichtungen vereinbaren die Parteien hiermit, dass die nachstehenden Bedingungen als Anhang zum Vertrag hinzugefügt werden.

1. **Begriffsbestimmungen**

„**Kundenpersonenbezogene** Daten“ bezeichnet personenbezogene Daten, die vom Unternehmen im Auftrag des Kunden im Rahmen der Bereitstellung der Produkte und/oder Dienstleistungen verarbeitet werden.

„CCPA“ bezeichnet den California Consumer Privacy Act in der durch den California Privacy Rights Act oder weitere kalifornische Gesetze/Vorschriften geänderten Fassung.

„**Betroffene** Person“ bezeichnet die Person, auf die sich die personenbezogenen Daten des Kunden beziehen.

„Datenschutzrahmenwerk“ oder „DPF“ bezeichnet den Rechtsrahmen der EU und der USA für die grenzüberschreitende Übermittlung personenbezogener Daten zwischen der Europäischen Union und den Vereinigten Staaten und umfasst die Erweiterung des DPF zwischen der EU und den USA auf das Vereinigte Königreich sowie das DPF zwischen der Schweiz und den USA.

„Datenschutzgesetze“ bezeichnet alle geltenden Gesetze und Vorschriften in Bezug auf die Verarbeitung personenbezogener Daten und den Datenschutz, die in den jeweiligen Rechtsordnungen bestehen, einschließlich, soweit anwendbar, der Datenschutz-Grundverordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr sowie zur Aufhebung der Richtlinie 95/46/EG („DSGVO“) (und alle Änderungen oder Ersetzungen davon), das Schweizer Bundesgesetz über den Datenschutz („FADP“) (und alle Änderungen oder Ersetzungen davon), die EU-DSGVO in der geänderten Fassung und in das britische Recht gemäß dem UK European Union (Withdrawal) Act 2018 und den gemäß diesem Gesetz erlassenen sekundären Rechtsvorschriften („UK-DSGVO“) (und alle Änderungen oder Ersetzungen davon), das kanadische Gesetz zum Schutz personenbezogener Daten und elektronischer

Dokumente („PIPEDA“) (und alle Änderungen oder Ersetzungen davon), das brasilianische allgemeine Datenschutzgesetz („LGPD“) (und alle Änderungen oder Ersetzungen davon), das australische Datenschutzgesetz von 1988 (Cth) in seiner geänderten Fassung („australisches Datenschutzgesetz“) (und alle Änderungen oder Ersetzungen davon), US-amerikanische Datenschutzgesetze der Bundesstaaten (einschließlich des CCPA und CPRA von Kalifornien) in ihrer jeweils gültigen Fassung oder alle anderen geltenden Datenschutzgesetze, die eine DPA erfordern. Wenn die DSGVO ausdrücklich erwähnt wird, gelten die gleichen Anforderungen für alle anderen gleichwertigen Anforderungen anderer geltender Datenschutzgesetze.

„**Personenbezogene** Daten“ sind alle Informationen, die sich auf eine betroffene Person beziehen, einschließlich, aber nicht beschränkt auf Namen, Identifikationsnummern, Standortdaten, Online-Kennungen oder ein oder mehrere spezifische Merkmale, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität der betroffenen Person sind.

„Verarbeitung“ bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten von Kunden, wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder jede andere Veränderung, das Auslesen, das Abrufen, die Verwendung, die Offenlegung durch Übermittlung, die Speicherung oder ein anderes Verfahren, das Einbeziehung personenbezogener Daten von Kunden, das Erstellen von Profilen, das Kombinieren von Daten aus verschiedenen Quellen, das Schließen von Schlussfolgerungen über die betroffene Person oder jede andere Verwendung dieser Daten.

„Sicherheitsverletzung“ bezeichnet eine bestätigte Verletzung der Sicherheit, die zu einer versehentlichen oder unrechtmäßigen Zerstörung, zum Verlust, zur Veränderung, zur unbefugten Offenlegung oder zum unbefugten Zugriff auf übermittelte, gespeicherte oder anderweitig verarbeitete personenbezogene Daten des Kunden führt.

„Standardvertragsklauseln“ oder „SCCs“ bezeichnet die Standardvertragsklauseln, die gemäß den geltenden Datenschutzgesetzen festgelegt wurden (EU-Standardvertragsklauseln, iberoamerikanische Mustervertragsklauseln für internationale Übermittlungen personenbezogener Daten, ASEAN-Mustervertragsklauseln für grenzüberschreitende Datenübermittlungen, Hongkong-Mustervertragsklauseln für die grenzüberschreitende Übermittlung personenbezogener Daten, SDAIA-Standardvertragsklauseln für die Übermittlung personenbezogener Daten usw.).

„**Dritter**“ bezeichnet eine andere Partei als den Kunden oder das Unternehmen.

Die in dieser DPA verwendeten Begriffe „Verantwortlicher“, „Auftragsverarbeiter“ und „Aufsichtsbehörde“ haben die ihnen in den geltenden Datenschutzgesetzen zugewiesene Bedeutung.

Alle anderen nicht definierten, aber großgeschriebenen Begriffe haben die in der Vereinbarung oder dem geltenden Datenschutzgesetz festgelegte Bedeutung.

2. Verarbeitung personenbezogener Daten des Kunden

- 2.1 Zweck der Verarbeitung. Der Zweck der Datenverarbeitung gemäß dieser DPA ist die Bereitstellung der Produkte und/oder Dienstleistungen gemäß der Vereinbarung. Anhang 1 beschreibt den Gegenstand und die Einzelheiten der Verarbeitung personenbezogener Kundendaten.
- 2.2 Verantwortlichkeiten des Auftragsverarbeiters und des Verantwortlichen. Die Parteien erkennen an und vereinbaren, dass: (a) das Unternehmen ein Auftragsverarbeiter von personenbezogenen Daten des Kunden gemäß den Datenschutzgesetzen ist; (b) der Kunde ein Verantwortlicher für personenbezogene Daten des Kunden gemäß den Datenschutzgesetzen ist; (c) der Kunde für die Einholung aller erforderlichen Genehmigungen und Zustimmungen für die Eingabe, Nutzung, Bereitstellung, Speicherung und Verarbeitung der personenbezogenen Daten des Kunden verantwortlich ist, damit das Unternehmen die Produkte und/oder Dienstleistungen bereitstellen kann; und (d) jede Partei die ihr gemäß den Datenschutzgesetzen obliegenden Verpflichtungen in Bezug auf die Verarbeitung der personenbezogenen Daten des Kunden einhält.
- 2.3 US-Datenschutzgesetze. Für die Zwecke der US-Datenschutzgesetze (einschließlich des CCPA) umfasst „Verantwortlicher“ „Unternehmen“, „Auftragsverarbeiter“ umfasst „Dienstleister“, „betroffene Person“ umfasst „Verbraucher“ und „personenbezogene Daten“ umfasst „personenbezogene Informationen“. Das Unternehmen ist ein Dienstleister und der Kunde ist ein Unternehmen.
- 2.4 Anweisungen des Kunden. Der Kunde weist das Unternehmen an, personenbezogene Daten des Kunden zu verarbeiten: (a) in Übereinstimmung mit der Vereinbarung und allen geltenden Ergänzungen; (b) soweit dies anderweitig erforderlich ist, um die Produkte und/oder Dienstleistungen für den Kunden bereitzustellen; (c) soweit dies zur Einhaltung geltender Gesetze oder Vorschriften erforderlich ist; und (d) zur Einhaltung anderer angemessener schriftlicher Anweisungen des Kunden, sofern diese Anweisungen mit den Bestimmungen der Vereinbarung vereinbar sind. Der Kunde stellt sicher, dass seine Anweisungen zur Verarbeitung der personenbezogenen Daten des Kunden den Datenschutzgesetzen entsprechen. Im Verhältnis zwischen den Parteien ist der Kunde allein verantwortlich für die Richtigkeit, Qualität und Rechtmäßigkeit der personenbezogenen Daten des Kunden und die Mittel, mit denen der Kunde die personenbezogenen Daten des Kunden erhalten hat.
- 2.5 Einhaltung der Anweisungen des Kunden durch das Unternehmen. Das Unternehmen verarbeitet personenbezogene Daten des Kunden nur gemäß den Anweisungen des Kunden und behandelt personenbezogene Daten des Kunden als vertrauliche Informationen. Wenn das Unternehmen der Ansicht ist oder Kenntnis erlangt, dass eine Anweisung des Kunden im Widerspruch zu Datenschutzgesetzen steht, informiert das Unternehmen den Kunden innerhalb einer angemessenen Frist. Das Unternehmen kann personenbezogene Daten des Kunden auch ohne schriftliche Anweisung des Kunden verarbeiten, wenn dies nach den für das Unternehmen geltenden Gesetzen erforderlich ist. In diesem Fall informiert das Unternehmen den Kunden über diese Anforderung, bevor es die personenbezogenen Daten des Kunden verarbeitet, sofern dies nicht durch geltendes Recht untersagt ist.

- 2.6 Verarbeitung gemäß CCPA. Soweit die Verarbeitung personenbezogener Daten durch das Unternehmen dem CCPA unterliegt, versichert das Unternehmen, dass es nicht (a) personenbezogene Daten des Kunden auf andere Weise als in der Vereinbarung vorgesehen, zur Bereitstellung der Produkte und/oder Dienstleistungen, zur Verbesserung der Qualität der Produkte und/oder Dienstleistungen, zur Aufdeckung von Sicherheitsvorfällen, zum Schutz vor betrügerischen oder illegalen Aktivitäten, zur Beauftragung von Unterauftragsverarbeitern gemäß dieser DPA oder in anderweitig durch den CCPA zulässiger Weise speichern, verwenden oder offenlegen; oder (b) personenbezogene Daten des Kunden verkaufen oder weitergeben.

3. Unterauftragsverarbeiter

- 3.1 Beauftragung von Unterauftragsverarbeitern. Der Kunde erteilt hiermit der Gesellschaft eine allgemeine schriftliche Genehmigung, Drittunterauftragsverarbeiter mit der Erbringung begrenzter oder ergänzender Dienstleistungen im Zusammenhang mit der Bereitstellung von Produkten und/oder Dienstleistungen zu beauftragen. Auf der Website des Unternehmens sind die Unterauftragsverarbeiter aufgeführt, die derzeit vom Unternehmen mit der Durchführung bestimmter Verarbeitungsaktivitäten im Zusammenhang mit personenbezogenen Daten des Kunden beauftragt sind (<https://commandalkon.com/sub-processor-list/>). Das Unternehmen aktualisiert die Liste der Unterauftragsverarbeiter, bevor es neue Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungsaufgaben beauftragt. Der Kunde kann sich jederzeit für elektronische Updates anmelden, wenn die Liste der Unterauftragsverarbeiter des Unternehmens geändert wird, indem er eine entsprechende Anfrage auf der Seite des Unternehmens für Unterauftragsverarbeiter (siehe Link oben) stellt oder eine solche Anfrage an privacy@commandalkon.com sendet. Der Kunde kann jedem Unterauftragsverarbeiter widersprechen, indem er diesen Widerspruch innerhalb von dreißig (30) Tagen nach einer Aktualisierung dem Unternehmen mitteilt, und die Parteien werden sich in gutem Glauben bemühen, den Widerspruch auszuräumen. Der Kunde erklärt sich hiermit mit den Unterauftragsverarbeitungsaktivitäten der aktuellen Unterauftragsverarbeiter einverstanden, die auf der Website des Unternehmens aufgeführt sind.
- 3.2 Sicherheit der Unterauftragsverarbeiter. Wenn das Unternehmen seine Verpflichtungen untervergeben, darf es dies nur im Rahmen einer schriftlichen Vereinbarung mit dem Unterauftragsverarbeiter tun, die diesem vertragliche Verpflichtungen auferlegt, die mindestens denen entsprechen, die dem Unternehmen gemäß dieser DPA auferlegt sind. Die Parteien vereinbaren, dass Kopien der Vereinbarungen mit autorisierten Unterauftragsverarbeitern, die gemäß den geltenden Standardvertragsklauseln zur Verfügung gestellt werden müssen, nur auf schriftliche Anfrage des Kunden zur Verfügung gestellt werden.
- 3.3 Haftung. Wenn der Unterauftragsverarbeiter seinen Datenschutzverpflichtungen gemäß einer solchen schriftlichen Vereinbarung nicht nachkommt, bleibt das Unternehmen gegenüber dem Kunden in vollem Umfang für die Erfüllung der Verpflichtungen des Unterauftragsverarbeiters gemäß dieser Vereinbarung haftbar.

4. Verantwortlichkeiten für Sicherheits en

- 4.1 Sicherheit des Unternehmens. Das Unternehmen wird unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Art und der Zwecke der Verarbeitung sowie des Risikos der unterschiedlichen Wahrscheinlichkeit und Schwere für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten des Kunden („ ssicherheitsprogramm“) implementieren. Das Unternehmen unterliegt den folgenden Sicherheitsstandards: SOC 2; NIST 800-171; AWS CIS.
- 4.2 Kundensicherheit. Der Kunde erkennt an, dass die Produkte und/oder Dienstleistungen bestimmte Merkmale und Funktionen enthalten, deren Nutzung der Kunde wählen kann und die sich auf die Sicherheit der personenbezogenen Daten des Kunden auswirken, die durch die Nutzung der Produkte und/oder Dienstleistungen durch den Kunden verarbeitet werden. Der Kunde ist dafür verantwortlich, die vom Unternehmen zur Verfügung gestellten Informationen zur Datensicherheit zu überprüfen und unabhängig zu entscheiden, ob die Produkte und/oder Dienstleistungen den Anforderungen und gesetzlichen Verpflichtungen des Kunden entsprechen, einschließlich seiner Verpflichtungen gemäß den geltenden Datenschutzgesetzen. Der Kunde ist ferner dafür verantwortlich, die Produkte und/oder Dienstleistungen ordnungsgemäß zu konfigurieren und die vom Unternehmen zur Verfügung gestellten Features und Funktionen zu nutzen, um eine angemessene Sicherheit unter Berücksichtigung der Art der personenbezogenen Daten des Kunden zu gewährleisten, die aufgrund der Nutzung der Produkte und/oder Dienstleistungen durch den Kunden verarbeitet werden. Der Kunde ist für die Nutzung der Produkte und/oder Dienstleistungen und die Speicherung von Kopien der personenbezogenen Daten des Kunden außerhalb der Systeme des Unternehmens oder der Unterauftragsverarbeiter des Unternehmens verantwortlich, einschließlich, aber nicht beschränkt auf die Sicherung der Anmeldedaten, Systeme und Geräte sowie die Aufbewahrung von Kopien seiner personenbezogenen Daten des Kunden in angemessener Weise.
- 4.3 Unternehmenspersonal. Das Unternehmen stellt sicher, dass sein mit der Verarbeitung von personenbezogenen Kundendaten befasstes Personal über die Vertraulichkeit der personenbezogenen Kundendaten informiert ist, eine angemessene Schulung hinsichtlich seiner Verantwortlichkeiten erhalten hat und der Geheimhaltungspflicht unterliegt, wobei diese Verpflichtungen auch nach Beendigung des Arbeitsverhältnisses mit dem Unternehmen bestehen bleiben.
- 4.4 Sicherheitstests. Das Unternehmen testet, bewertet und evaluiert die Wirksamkeit des Informationssicherheitsprogramms zur Gewährleistung der sicheren Verarbeitung von personenbezogenen Daten des Kunden. Das Unternehmen hält sich an sein Informationssicherheitsprogramm und versichert und garantiert, dass sein Informationssicherheitsprogramm den geltenden Gesetzen entspricht und auch in Zukunft entsprechen wird.
- 4.5 Folgenabschätzungen. Das Unternehmen ergreift angemessene Maßnahmen, um den Kunden bei der Durchführung von Folgenabschätzungen und damit verbundenen

Konsultationen mit Aufsichtsbehörden zu unterstützen, wenn der Kunde gemäß den Datenschutzgesetzen zur Durchführung solcher Folgenabschätzungen verpflichtet ist.

5. Rechte der betroffenen Personen

- 5.1 Unterstützung bei den Pflichten des Kunden. Soweit der Kunde bei der Nutzung oder dem Erhalt der Produkte und/oder Dienstleistungen nicht in der Lage ist, personenbezogene Daten des Kunden gemäß den Datenschutzgesetzen zu korrigieren, zu ändern, einzuschränken, zu sperren oder zu löschen, wird das Unternehmen unverzüglich auf angemessene Anfragen des Kunden hin solche Maßnahmen ermöglichen, soweit dies gesetzlich zulässig und möglich ist. Soweit gesetzlich zulässig, trägt der Kunde alle Kosten, die dem Unternehmen durch die Bereitstellung dieser Unterstützung entstehen.
- 5.2 Benachrichtigungspflichten. Das Unternehmen wird den Kunden, soweit gesetzlich zulässig, unverzüglich benachrichtigen, wenn es eine Anfrage einer betroffenen Person auf Zugang, Berichtigung, Änderung, Löschung oder Widerspruch gegen die Verarbeitung von personenbezogenen Daten des Kunden erhält, die sich auf diese Person beziehen. Das Unternehmen wird ohne vorherige schriftliche Zustimmung des Kunden nicht auf solche Anfragen betroffener Personen in Bezug auf personenbezogene Daten des Kunden reagieren, es sei denn, um zu bestätigen, dass die Anfrage den Kunden betrifft. Darüber hinaus wird das Unternehmen, soweit gesetzlich zulässig, den Kunden unverzüglich benachrichtigen, wenn es eine Anfrage zur Offenlegung oder Korrespondenz, eine Mitteilung oder sonstige Kommunikation in Bezug auf personenbezogene Daten des Kunden von Strafverfolgungsbehörden, einer zuständigen Behörde oder einer zuständigen Datenschutzbehörde erhält. Das Unternehmen wird dem Kunden im Rahmen des gesetzlich Zulässigen und soweit der Kunde durch die Nutzung oder den Erhalt der Produkte und/oder Dienstleistungen keinen Zugriff auf diese personenbezogenen Daten des Kunden hat, bei der Bearbeitung solcher Anfragen in angemessener Weise kooperieren und unterstützen. Soweit gesetzlich zulässig, trägt der Kunde alle Kosten, die dem Unternehmen durch die Bereitstellung dieser Unterstützung entstehen.

6. Verletzung des Schutzes personenbezogener Daten

- 6.1 Benachrichtigungspflichten. Wenn das Unternehmen Kenntnis von einer bestätigten Sicherheitsverletzung in Bezug auf personenbezogene Daten des Kunden erhält, wird das Unternehmen den Kunden unverzüglich, spätestens jedoch innerhalb von zweiundsiebzig (72) Stunden nach der Bestätigung, über die Sicherheitsverletzung informieren. Die Verpflichtungen in diesem Abschnitt 6 gelten nicht für Vorfälle, die durch den Kunden oder dessen Mitarbeiter oder Endnutzer verursacht wurden, oder für erfolglose Versuche oder Aktivitäten, die die Sicherheit der personenbezogenen Daten des Kunden nicht gefährden, einschließlich erfolgloser Anmeldeversuche, Pings, Port-Scans, Denial-of-Service-Angriffe und anderer Netzwerkangriffe auf Firewalls oder vernetzte Systeme.
- 6.2 Art der Benachrichtigung. Die Benachrichtigung über Sicherheitsverletzungen erfolgt per E-Mail oder telefonisch an den Ansprechpartner des Kunden. Es liegt in der alleinigen Verantwortung des Kunden, sicherzustellen, dass seine Kontaktdaten in den Support-Systemen des Unternehmens jederzeit korrekt sind. Der Kunde ist allein

verantwortlich für die Einhaltung der für ihn geltenden Meldepflichten bei Sicherheitsverletzungen und die Erfüllung aller Verpflichtungen zur Benachrichtigung Dritter im Zusammenhang mit einer Verletzung der Sicherheit personenbezogener Daten.

- 6.3 Inhalt der Benachrichtigung. Wenn eine Benachrichtigung erforderlich ist, muss diese mindestens und soweit verfügbar Folgendes enthalten:
- 6.3.1 eine Beschreibung der Art der Sicherheitsverletzung, der Kategorien und Anzahl der betroffenen Personen sowie der Kategorien und Anzahl der betroffenen personenbezogenen Daten;
 - 6.3.2 den Namen und die Kontaktdaten des zuständigen Ansprechpartners des Unternehmens, von dem weitere Informationen eingeholt werden können;
 - 6.3.3 die wahrscheinlichen Folgen der Sicherheitsverletzung zu beschreiben; und
 - 6.3.4 die Maßnahmen beschreiben, die ergriffen wurden oder geplant sind, um die Sicherheitsverletzung zu beheben.

7. **Löschung oder Rückgabe personenbezogener Kundendaten**

- 7.1 Löschen oder Zurückgeben. Vorbehaltlich Abschnitt 7.3 verpflichtet sich das Unternehmen, unverzüglich und in jedem Fall innerhalb von dreißig (30) Tagen nach Beendigung aller Dienste, die die Verarbeitung personenbezogener Kundendaten umfassen (das „Beendigungsdatum“), personenbezogene Kundendaten sicher zu löschen oder auf rechtzeitige schriftliche Anfrage des Kunden eine vollständige Kopie aller personenbezogenen Kundendaten an den Kunden durch sichere Dateiübertragung in einem vom Kunden angemessen geforderten Format zurückzugeben.
- 7.2 Schriftliche Bestätigung. Wenn der Kunde und das Unternehmen Standardvertragsklauseln vereinbart haben, die eine schriftliche Bestätigung der Löschung erfordern (wie Klauseln 8.5 und 16 der EU-SCC), vereinbaren die Parteien, dass eine schriftliche Bestätigung nur auf schriftliche Anfrage des Kunden erteilt wird.
- 7.3 Definition von „Löschen“. Zur Klarstellung: „Löschen“ bedeutet, personenbezogene Daten des Kunden so zu entfernen oder zu vernichten, dass sie nicht wiederhergestellt oder rekonstruiert werden können.
- 7.4 Aufzeichnungen. Das Unternehmen kann personenbezogene Daten des Kunden in dem Umfang aufbewahren, der nach geltendem Recht erforderlich ist oder in den Aufbewahrungsfristen des Unternehmens vorgesehen ist, vorausgesetzt, dass das Unternehmen die Vertraulichkeit aller dieser personenbezogenen Daten des Kunden gewährleistet.

8. Rechte auf Audit-

- 8.1 Prüfungsrechte. Der Kunde kann höchstens einmal pro Jahr einen gemeinsam vereinbarten Dritten mit der Prüfung der Unternehmensdaten beauftragen, und zwar ausschließlich zum Zweck der Erfüllung seiner Prüfungsanforderungen gemäß Artikel 28 Absatz 3 Buchstabe h der DSGVO oder einer gleichwertigen Bestimmung des geltenden Datenschutzrechts. Um eine Prüfung zu beantragen, muss der Kunde mindestens vier (4) Wochen vor dem vorgeschlagenen Prüfungstermin einen detaillierten Prüfungsplan vorlegen, in dem der vorgeschlagene Umfang, die Dauer und der Beginn der Prüfung beschrieben sind. Audit-Anfragen sind an anprivacy@commandalkon.com zu senden. Der Auditor muss vor Durchführung des Audits eine für das Unternehmen akzeptable schriftliche Vertraulichkeitsvereinbarung unterzeichnen. Das Audit muss während der regulären Geschäftszeiten gemäß den Richtlinien des Unternehmens durchgeführt werden und darf die Geschäftstätigkeit des Unternehmens nicht unangemessen beeinträchtigen. Alle Audits gehen ausschließlich zu Lasten und auf Kosten des Kunden. Das Unternehmen wird mit jedem Kunden oder jeder zuständigen Regulierungs- oder Aufsichtsbehörde bei der Überprüfung der Einhaltung seiner Verpflichtungen aus dieser DPA kooperieren, indem es vorbehaltlich der Geheimhaltungspflichten, sofern verfügbar, Auditberichte Dritter und/oder Beschreibungen der Sicherheitskontrollen und andere vom Kunden angemessen angeforderte Informationen über die Sicherheitspraktiken und -richtlinien des Unternehmens zur Verfügung stellt.
- 8.2 Unterstützung bei der Einhaltung. Unter Berücksichtigung der Art der Verarbeitung und der dem Unternehmen zur Verfügung stehenden Informationen wird das Unternehmen dem Kunden angemessene und zumutbare Unterstützung und Mitwirkung bei der Erfüllung seiner Verpflichtungen gemäß den Artikeln 32 bis 36 der DSGVO gewähren.

9. Datenübermittlungen

- 9.1 Allgemeine Genehmigung. Der Kunde erklärt sich damit einverstanden, dass das Unternehmen vorbehaltlich Abschnitt 9.2 personenbezogene Daten des Kunden in den Vereinigten Staaten von Amerika und jedem anderen Land, in dem das Unternehmen oder einer seiner Unterauftragsverarbeiter Einrichtungen unterhält oder anderweitig personenbezogene Daten verarbeitet, speichern und verarbeiten darf. Jede solche Übermittlung unterliegt in erster Linie der Datenschutz-Framework-Zertifizierung des Unternehmens oder alternativ den Standardvertragsklauseln des Unternehmens für verbundene Unternehmen. Das Unternehmen wird keine personenbezogenen Daten des Kunden von einer Gerichtsbarkeit in eine andere übertragen oder deren Übertragung veranlassen, es sei denn, dies geschieht in Übereinstimmung mit geltendem Recht, und wird nicht dazu führen, dass der Kunde gegen Datenschutzgesetze verstößt.
- 9.2 EU-Standardvertragsklauseln. Soweit und nur insoweit das Unternehmen personenbezogene Daten von Kunden aus dem Europäischen Wirtschaftsraum verarbeitet und Standardvertragsklauseln erforderlich sind, gelten die Standardvertragsklauseln in Modul Zwei, die hiermit Bestandteil dieser Vereinbarung

werden. Für die Zwecke der Standardvertragsklauseln ist der Kunde der „Datenexporteur“ und das Unternehmen der „Datenimporteur“.

- 9.3 Anhang für das Vereinigte Königreich zu den EU-Standardvertragsklauseln. Soweit und nur insoweit das Unternehmen personenbezogene Daten von Kunden aus dem Vereinigten Königreich verarbeitet und Standardvertragsklauseln erforderlich sind, vereinbaren die Parteien, dass der britische Nachtrag für personenbezogene Daten gilt, die über die Produkte und/oder Dienstleistungen aus dem Vereinigten Königreich entweder direkt oder über eine Weiterübermittlung an ein Land oder einen Empfänger außerhalb des Vereinigten Königreichs übermittelt werden, das bzw. der von der zuständigen britischen Regulierungsbehörde oder Regierungsstelle für das Vereinigte Königreich nicht als Land anerkannt ist, das ein angemessenes Schutzniveau für personenbezogene Daten bietet.
- 9.4 Schweizerisches Bundesgesetz über den Datenschutz (FADP). Soweit und nur insoweit das Unternehmen personenbezogene Daten von Kunden aus der Schweiz verarbeitet, gelten die folgenden zusätzlichen Anforderungen, sofern die Datenübermittlungen ausschließlich dem FADP oder sowohl dem FADP als auch der EU-DSGVO unterliegen: (a) Der Begriff „Mitgliedstaat“ darf nicht so ausgelegt werden, dass betroffene Personen in der Schweiz von der Möglichkeit ausgeschlossen werden, ihre Rechte an ihrem gewöhnlichen Aufenthaltsort (Schweiz) gemäß Klausel 18(c) der Standardvertragsklauseln geltend zu machen. (b) Soweit die den Standardvertragsklauseln zugrunde liegenden Datenübermittlungen ausschließlich dem FADP unterliegen, sind Verweise auf die EU-DSGVO als Verweise auf das FADP zu verstehen. und (c) soweit die den Standardvertragsklauseln zugrunde liegenden Datenübermittlungen sowohl dem FADP als auch der EU-DSGVO unterliegen, sind Verweise auf die EU-DSGVO als Verweise auf das FADP zu verstehen, soweit die Datenübermittlungen dem FADP unterliegen.
- 9.5 Andere Standardvertragsklauseln oder Mustervertragsklauseln. Soweit und nur insoweit eine Übermittlung von personenbezogenen Daten des Kunden erfolgt, die nicht unter die oben genannten Bestimmungen fällt und gemäß den geltenden Datenschutzgesetzen länderspezifische SCC oder Mustervertragsklauseln erfordert, vereinbaren die Parteien, dass die entsprechenden erforderlichen länderspezifischen SCC oder Mustervertragsklauseln hiermit automatisch durch Verweis aufgenommen werden und integraler Bestandteil dieser DPA sind.
- 9.6 Ergänzende Maßnahmen. Ergänzend zu den Standardvertragsklauseln gilt Folgendes: Wenn das Unternehmen Kenntnis davon erlangt, dass eine staatliche Behörde (einschließlich Strafverfolgungsbehörden) aus Gründen der nationalen Sicherheit freiwillig oder zwangsweise Zugang zu einigen oder allen vom Unternehmen verarbeiteten personenbezogenen Daten des Kunden oder eine Kopie davon erhalten möchte, wird das Unternehmen, sofern dies nicht gesetzlich verboten ist oder einer zwingenden gesetzlichen Verpflichtung unterliegt, die etwas anderes vorschreibt, 1) den Kunden, auf den sich die personenbezogenen Daten beziehen, unverzüglich benachrichtigen; 2) die zuständige staatliche Behörde darüber informieren, dass sie nicht zur Offenlegung der personenbezogenen Daten des Kunden berechtigt ist und, sofern nicht gesetzlich verboten, den Kunden, auf den sich die personenbezogenen Daten des Kunden beziehen, unverzüglich benachrichtigen muss; 3) die

Regierungsbehörde darüber informieren, dass sie alle Anfragen oder Forderungen direkt an den Kunden richten soll, auf den sich die personenbezogenen Daten des Kunden beziehen; und 4) keinen Zugriff auf die personenbezogenen Daten des Kunden gewähren, bis der Kunde, auf den sich die personenbezogenen Daten des Kunden beziehen, schriftlich seine Zustimmung erteilt hat oder bis das Unternehmen gesetzlich dazu verpflichtet ist. Wenn das Unternehmen gesetzlich dazu verpflichtet ist, wird es angemessene und rechtmäßige Anstrengungen unternehmen, um eine solche Untersagung oder Verpflichtung anzufechten. Wenn das Unternehmen zur Herausgabe der personenbezogenen Daten des Kunden verpflichtet ist, wird das Unternehmen die personenbezogenen Daten des Kunden nur in dem Umfang offenlegen, in dem dies gemäß den geltenden Rechtsvorschriften erforderlich ist.

- 9.7 Auslandsgeheimdienstgesetz (Foreign Intelligence Surveillance Act). Das Unternehmen hat bisher keine Anweisung gemäß Abschnitt 702 des US-Auslandsgeheimdienstgesetzes (Foreign Intelligence Surveillance Act), kodifiziert in 50 U.S.C. §1881a („FISA Abschnitt 702“), erhalten. Kein Gericht hat festgestellt, dass das Unternehmen zu den Einrichtungen gehört, die gemäß FISA Section 702 zur Erhalt von Verfahren berechtigt sind. Das Unternehmen gehört nicht zu den Anbietern, die gemäß FISA Section 702, wie in der *Schrems-II*-Entscheidung beschrieben, zur Upstream-Erhebung („Massenerhebung“) berechtigt sind.
- 9.8 Vorrang der Übermittlung. Für den Fall, dass Dienstleistungen durch mehr als einen Übermittlungsmechanismus abgedeckt sind, unterliegt die Übermittlung der personenbezogenen Daten des Kunden einem einzigen Übermittlungsmechanismus in der folgenden Rangfolge: (i) Datenschutz-Framework-Zertifizierung des Unternehmens; (ii) geltende Standardvertragsklauseln (sofern nach geltendem Datenschutzrecht erforderlich).

10. Laufzeit und Kündigung

Laufzeit der DPA. Diese DPA tritt am Tag des vollständigen Inkrafttretens der Vereinbarung in Kraft und bleibt ungeachtet des Ablaufs der Laufzeit eines erworbenen Abonnements bis zur Löschung aller personenbezogenen Daten des Kunden gemäß dieser DPA in Kraft und erlischt automatisch mit deren Löschung.

11. Nichteinhaltung; Rechtsbehelfe; Parteien

- 11.1 Haftungsbeschränkung. Die Haftung des Unternehmens für Verstöße gegen seine Verpflichtungen aus dieser DPA unterliegt den Haftungsbeschränkungen in der Vereinbarung.
- 11.2 Vertragsparteien dieser DPA. Keine Bestimmung dieser DPA gewährt Personen oder Organisationen, die nicht Vertragsparteien dieser DPA sind, Vorteile oder Rechte.

12. Allgemeine

Anwendbares Recht und Gerichtsstand

- 12.1 Diese DPA wird unter Berücksichtigung der Umstände gegebenenfalls überprüft.

- 12.2 Unbeschadet der Klauseln 7 (Mediation und Gerichtsstand) und 9 (Anwendbares Recht) der Standardvertragsklauseln
- 12.2.1 unterwerfen sich die Parteien dieser DPA hiermit der in der Vereinbarung festgelegten Gerichtsbarkeit für alle Streitigkeiten oder Ansprüche, die sich aus dieser DPA ergeben , einschließlich Streitigkeiten über deren Bestehen, Gültigkeit oder Beendigung; und
- 12.2.2 Diese DPA und alle nicht vertraglichen oder sonstigen Verpflichtungen, die sich aus oder im Zusammenhang mit ihr ergeben, unterliegen den Gesetzen des Landes oder Gebiets, das zu diesem Zweck in der Vereinbarung festgelegt wurde.

Rangfolge

- 12.3 Im Falle von Widersprüchen oder Unstimmigkeiten zwischen dieser DPA und den Standardvertragsklauseln, sofern diese erforderlich sind, haben die Standardvertragsklauseln Vorrang.
- 12.4 Vorbehaltlich der Abschnitte 12.2 und 12.3 gelten in Bezug auf den Gegenstand dieser DPA im Falle von Unstimmigkeiten zwischen den Bestimmungen dieser DPA und anderen Vereinbarungen zwischen den Parteien, einschließlich der Vereinbarung und einschließlich (sofern nicht ausdrücklich schriftlich anders vereinbart und im Namen der Parteien unterzeichnet) Vereinbarungen, die nach dem Datum dieser DPA geschlossen wurden oder geschlossen werden sollen, die Bestimmungen dieser DPA.

Änderungen der Datenschutzgesetze

- 12.5 Der Kunde kann:
- 12.5.1 durch schriftliche Mitteilung an das Unternehmen mit einer Frist von mindestens dreißig (30) Kalendertagen von Zeit zu Zeit Änderungen der Standardvertragsklauseln vorschlagen, die aufgrund einer Änderung des Datenschutzgesetzes oder einer Entscheidung einer zuständigen Behörde gemäß diesem Datenschutzgesetz erforderlich sind; und
- 12.5.2 alle sonstigen Änderungen dieser DPA vorschlagen, die der Kunde nach vernünftigem Ermessen für erforderlich hält, um den Anforderungen eines Datenschutzgesetzes nachzukommen.
- 12.6 Wenn der Kunde eine Mitteilung gemäß Abschnitt 12.5 macht, werden die Parteien die vorgeschlagenen Änderungen unverzüglich erörtern und in gutem Glauben verhandeln, um diese oder alternative Änderungen, die den in der Mitteilung des Kunden genannten Anforderungen entsprechen, so schnell wie möglich zu vereinbaren und umzusetzen.

Salvatorische

- 12.7 Sollte eine Bestimmung dieser DPA ungültig oder nicht durchsetzbar sein, bleibt der Rest dieser DPA gültig und in Kraft. Die ungültige oder nicht durchsetzbare

Bestimmung wird entweder (i) so geändert, dass ihre Gültigkeit und Durchsetzbarkeit gewährleistet ist und die Absichten der Parteien so weit wie möglich gewahrt bleiben, oder, falls dies nicht möglich ist, (ii) so ausgelegt, als ob der ungültige oder nicht durchsetzbare Teil nie enthalten gewesen wäre.

Anhang I – Einzelheiten zur Datenverarbeitung

Datenexporteur (Verantwortlicher): Der in der Vereinbarung genannte Kunde.

Datenimporteur (Auftragsverarbeiter): Das in der Vereinbarung genannte Unternehmen.

Gegenstand: Gegenstand der Datenverarbeitung gemäß dieser DPA sind die personenbezogenen Daten des Kunden.

Dauer der Verarbeitung: Die Laufzeit der Vereinbarung zuzüglich des Zeitraums, bis das Unternehmen alle personenbezogenen Daten des Kunden gemäß dieser DPA löscht.

Zweck: Der Zweck der Datenverarbeitung ist die Bereitstellung der Produkte und/oder Dienstleistungen für den Kunden.

Art der Verarbeitung: Die Art der Datenverarbeitung dient der Bereitstellung der Produkte und/oder Dienstleistungen, wie in der Vereinbarung und dieser DPA beschrieben.

Kategorien der betroffenen Personen: Mitarbeiter des Kunden und Mitarbeiter von verbundenen Unternehmen des Kunden, Kunden und Geschäftspartner.

Arten personenbezogener Daten: Der Kunde kann bestimmte personenbezogene Daten des Kunden in die Produkte und/oder Dienstleistungen hochladen, übermitteln oder auf andere Weise bereitstellen, wobei der Umfang in der Regel vom Kunden nach eigenem Ermessen festgelegt und kontrolliert wird und Kontaktinformationen, Informationen zur Interaktion mit der Website, den Produkten und Dienstleistungen, Adressen, Geburtsdatum, Geburtsort, E-Mail-Adressen, Namen, Geschlecht, Titel, Telefonnummern, Führerscheinnummer, Unterschrift, Mitarbeiternummer, Geolokalisierungsdaten, Vergütung, Benutzername, Passwort, Leistungsdaten, Qualifikationen und Einschränkungen sowie Geräteinformationen.

Übertragene sensible Daten: Keine.

Häufigkeit der Übertragung: Kontinuierlich, soweit dies für die Bereitstellung der Produkte und/oder Dienstleistungen erforderlich ist.

Übermittlung an Unterauftragsverarbeiter: Wie in dieser DPA und der Liste der Unterauftragsverarbeiter des Unternehmens unter beschrieben. Aufzeichnungen über die Verarbeitungstätigkeiten sind auf Anfrage erhältlich.

Zuständige Aufsichtsbehörde: Wie durch die geltenden Datenschutzgesetze festgelegt oder, in der Reihenfolge ihrer Wirksamkeit, 1) gemäß den Bestimmungen der Vereinbarung oder 2) die Datenschutzbehörde der Niederlande.

Aufbewahrung: In Übereinstimmung mit der Vereinbarung und dieser DPA.

Technische und organisatorische Maßnahmen: Die vom Datenimporteur implementierten technischen und organisatorischen Sicherheitsmaßnahmen sind in Abschnitt 4.1 der DPA beschrieben. Weitere Details sind auf Anfrage erhältlich.